Office of Foreign Assets Control — Overview

Objective. *Assess the bank's risk-based Office of Foreign Assets Control (OFAC) program to evaluate whether it is appropriate for the bank's OFAC risk, taking into consideration its products, services, customers, transactions, and geographic locations.*

OFAC is an office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against entities such as targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, therefore, they are multilateral in scope, and involve close cooperation with allied governments. Other sanctions are specific to the interests of the United States. OFAC has been delegated responsibility by the Secretary of the Treasury for developing, promulgating, and administering U.S. sanctions programs.[119]

All U.S. persons,[120] including U.S. banks, bank holding companies, and non-bank subsidiaries, must comply with OFAC's regulations.[121] The federal banking agencies evaluate OFAC compliance systems to ensure that all banks subject to their supervision comply with the sanctions.[122] Unlike the BSA, the laws and OFAC-issued regulations apply not only to U.S. banks, their domestic branches, agencies, and international banking facilities, but also to their foreign branches, and often overseas offices and subsidiaries. In general, the regulations require the following:

---

[119] Trading With the Enemy Act (TWEA), 50 USC App 1-44; International Emergency Economic Powers Act (IEEPA), 50 USC 1701 *et seq.*; Antiterrorism and Effective Death Penalty Act (AEDPA), 8 USC 1189, 18 USC 2339B; United Nations Participation Act (UNPA), 22 USC 287c; Cuban Democracy Act (CDA), 22 USC 6001–10; The Cuban Liberty and Democratic Solidarity Act (Libertad Act), 22 USC 6021–91; The Clean Diamonds Trade Act, Pub. L. No. 108-19; Foreign Narcotics Kingpin Designation Act (Kingpin Act), 21 USC 1901–1908, 8 USC 1182; Burmese Freedom and Democracy Act of 2003, Pub. L. No. 108–61, 117 Stat. 864 (2003); The Foreign Operations, Export Financing and Related Programs Appropriations Act, Sec 570 of Pub. L. No. 104-208, 110 Stat. 3009-116 (1997); The Iraqi Sanctions Act, Pub. L. No. 101-513, 104 Stat. 2047-55 (1990); The International Security and Development Cooperation Act, 22 USC 2349 aa8–9; The Trade Sanctions Reform and Export Enhancement Act of 2000, Title IX, Pub. L. No. 106-387 (October 28, 2000).

[120] All U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the case of certain programs, such as those regarding Cuba and North Korea, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S. origin goods to comply.

[121] Additional information is provided in "Foreign Assets Control Regulations for the Financial Community," which is available on OFAC's web site www.treas.gov/ofac/.

[122] 31 CFR chapter V.

- Block accounts and other property of specified countries, entities, and individuals.
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.

Blocked Transactions

U.S. law requires that assets and accounts of an OFAC-specified country, entity, or individual be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. For example, if a funds transfer comes from offshore and is being routed through a U.S. bank to an offshore bank, and there is an OFAC-designated party on the transaction, it must be blocked. The definition of assets and property is broad and is specifically defined within each sanction program. Assets and property includes anything of direct, indirect, present, future, or contingent value (including all types of bank transactions). Banks must block transactions that:

- Are by or on behalf of a blocked individual or entity;
- Are to or go through a blocked entity; or
- Are in connection with a transaction in which a blocked individual or entity has an interest.

For example, if a U.S. bank receives instructions to make a funds transfer payment that falls into one of these categories, it must execute the payment order and place the funds into a blocked account.[123] A payment order cannot be canceled or amended after it is received by a U.S. bank in the absence of an authorization from OFAC.

Prohibited Transactions

In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction (i.e., the transaction should not be accepted, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected, (i.e., not processed). For example, the Sudanese Sanctions Regulations prohibit transactions in support of commercial activities in Sudan. Therefore, a U.S. bank would have to reject a funds transfer between two companies, which are not Specially Designated Nationals or Blocked Persons (SDNs), involving an export to a company in Sudan that also is not an SDN. Because Sudanese Sanctions would only require blocking transactions with the Government of Sudan or SDNs, there would be no blockable interest in the funds between the two companies. However, because the transactions would constitute support of Sudanese commercial activity, which is prohibited, the U.S. bank can not process the transaction and would simply reject the transaction.

[123] A blocked account is a segregated interest-bearing account (at a commercially reasonable rate), which holds the customer's property until the target is delisted, the sanctions program is rescinded, or the customer obtains an OFAC license authorizing the release of the property.

It is important to note that the OFAC regime specifying prohibitions against certain countries, entities, and individuals is separate and distinct from the provision within the BSA's Customer Identification Program (CIP) regulation (31 CFR 103.121) that requires banks to compare new accounts against government lists of known or suspected terrorists or terrorist organizations within a reasonable period of time after the account is opened. OFAC lists have not been designated government lists for purposes of the CIP rule. Refer to the core overview section, "Customer Identification Program," page 45, for further guidance. However, OFAC's requirements stem from other statutes not limited to terrorism, and OFAC sanctions apply to transactions, in addition to account relationships.

OFAC Licenses

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. OFAC can issue a license to engage in an otherwise prohibited transaction when it determines that the transaction does not undermine the U.S. policy objectives of the particular sanctions program, or is otherwise justified by U.S. national security or foreign policy objectives. OFAC can also promulgate general licenses, which authorize categories of transactions, such as allowing reasonable service charges on blocked accounts, without the need for case-by-case authorization from OFAC. These licenses can be found in the regulations for each sanctions program (31 CFR, Chapter V (Regulations)) and may be accessed from OFAC's web site. Before processing transactions that may be covered under a general license, banks should verify that such transactions meet the relevant criteria of the general license.[124]

Specific licenses are issued on a case-by-case basis.[125] A specific license is a written document issued by OFAC authorizing a particular transaction or set of transactions. To receive a specific license, the person or entity who would like to undertake the transaction must submit an application to OFAC. If the transaction conforms with U.S. foreign policy under a particular program, the license will be issued. If a bank's customer claims to have a specific license, the bank should verify that the transaction conforms to the terms of the license and obtain and retain a copy of the authorizing license.

OFAC Reporting

Banks must report all blockings to OFAC within ten days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30).[126] Once assets or funds are blocked, they should be placed in a blocked account. Prohibited transactions that are rejected must also be reported to OFAC within ten days of the occurrence.

---

[124] License information is available on OFAC's web site www.treas.gov/ofac, or by contacting OFAC's Licensing area at 202-622-2480.

[125] Specific licenses require an application directed to: Licensing Division, Office of Foreign Assets Control, 1500 Pennsylvania Avenue, NW, Washington, D.C. 20220.

[126] The annual report is to be filed on form TD F 90-22.50.

Banks must keep a full and accurate record of each rejected transaction for at least five years after the date of the transaction. For blocked property (including blocked transactions), records must be maintained for the period the property is blocked and for five years after the date the property is unblocked.

Additional information concerning OFAC regulations, such as Sanctions Program and Country Summaries brochures; the SDN list, including both entities and individuals; recent OFAC actions; and "Frequently Asked Questions," can be found on OFAC's web site.[127]

OFAC Program

While not required by specific regulation, but as a matter of sound banking practice and in order to ensure compliance, banks should establish and maintain an effective, written OFAC program commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). The program should identify high-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate a bank employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas of the bank. A bank's OFAC program should be commensurate with its respective OFAC risk profile.

OFAC Risk Assessment

A fundamental element of a sound OFAC program is the bank's assessment of its specific product lines, customer base, and nature of transactions and identification of the high-risk areas for OFAC transactions. The initial identification of high-risk customers for purposes of OFAC may be performed as part of the bank's CIP and CDD procedures. As OFAC sanctions can reach into virtually all areas of its operations, banks should consider all types of transactions, products, and services when conducting their risk assessment and establishing appropriate policies, procedures, and processes. An effective risk assessment should be a composite of multiple factors (as described in more detail below), and depending upon the circumstances, certain factors may be weighed more heavily than others.

Another consideration for the risk assessment is account and transaction parties. New accounts should be compared with OFAC lists prior to being opened or shortly thereafter. However, the extent to which the bank includes account parties other than accountholders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney) in the initial OFAC review during the account opening process, and during subsequent database reviews of existing accounts, will depend on the bank's risk profile and available technology.

[127] This information is available on OFAC's web site www.treas.gov/ofac, or by contacting OFAC's Hotline at 800-540-6322.

Based on the bank's OFAC risk profile for each area and available technology, the bank should establish policies, procedures, and processes for reviewing transactions and transaction parties (e.g., issuing bank, payee, endorser, or jurisdiction). Currently, OFAC provides guidance on transactions parties on checks. The guidance states if a bank knows or has reason to know that a transaction party on a check is an OFAC target, the bank's processing of the transaction would expose the bank to liability, especially personally handled transactions in a high-risk area. For example, if a bank knows or has a reason to know that a check transaction involves an OFAC-prohibited party or country, OFAC would expect timely identification and appropriate action.

In evaluating the level of risk, a bank should exercise judgment and take into account all indicators of risk. Although not an exhaustive list, examples of products, services, customers, and geographic locations that may carry a higher level of OFAC risk include:

- International funds transfers.
- Nonresident alien accounts.
- Foreign customer accounts.
- Cross-border automated clearing house (ACH) transactions.
- Commercial letters of credit.
- Transactional electronic banking.
- Foreign correspondent bank accounts.
- Payable through accounts.
- International private banking.
- Overseas branches or subsidiaries.

Appendix M ("Quantity of Risk — OFAC Procedures") provides guidance to examiners on assessing OFAC risks facing a bank. The risk assessment can be used to assist the examiner in determining the scope of the OFAC examination. Additional information on compliance risk is posted by OFAC on its web site under "Frequently Asked Questions."[128]

Once the bank has identified its areas with high OFAC risk, it should develop appropriate policies, procedures, and processes to address the associated risks. Banks may tailor these policies, procedures, and processes to the specific nature of a business line or product. Furthermore, banks are encouraged to periodically reassess their OFAC risks.

[128] This document is available at www.treas.gov/offices/enforcement/ofac/faq/#finance.

Internal Controls

An effective OFAC program should include internal controls for identifying suspect accounts and transactions and reporting to OFAC. Internal controls should include the following elements:

Identifying and reviewing suspect transactions. The bank's policies, procedures, and processes should address how the bank will identify and review transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software, or a combination of both. For screening purposes, the bank should clearly define its criteria for comparing names provided on the OFAC list with the names in the bank's files or on transactions and for identifying transactions or accounts involving sanctioned countries. The bank's policies, procedures, and processes should also address how it will determine whether an initial OFAC hit is a valid match or a false hit.[129] A high volume of false hits may indicate a need to review the bank's interdiction program.

The screening criteria used by banks to identify name variations and misspellings should be based on the level of OFAC risk associated with the particular product or type of transaction. For example, in a high-risk area with a high-volume of transactions, the bank's interdiction software should be able to identify close name derivations for review. The SDN list attempts to provide name derivations; however, the list may not include all derivations. More sophisticated interdiction software may be able to catch variations of an SDN's name not included on the SDN list. Low-risk banks or areas and those with low volumes of transactions may decide to manually filter for OFAC compliance. Decisions to use interdiction software and the degree of sensitivity of that software should be based on a bank's assessment of its risk and the volume of its transactions. In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), banks should consider the likelihood of incurring a violation and available technology. In addition, banks should periodically reassess their OFAC filtering system. For example, if a bank identifies a name derivation of an OFAC target, then OFAC suggests that the bank add the name to its filtering process.

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter (e.g., during nightly processing). Banks that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits, from occurring until the OFAC check is completed. Prohibited transactions conducted prior to completing an OFAC check may be subject to possible penalty action. In addition, banks should have policies, procedures, and processes in place to check existing customers when there are additions or changes to the OFAC list. The frequency of the review should be based on the bank's OFAC risk. For example, banks with a low OFAC risk level may periodically (e.g., monthly or quarterly) compare the customer base against the OFAC list. Transactions such as funds transfers, letters of credit, and noncustomer transactions should be checked against OFAC lists prior to being

[129] Due diligence steps for determining a valid match are provided in "Using OFAC's Hotline" on OFAC's web site www.treas.gov/ofac.

executed. When developing OFAC policies, procedures, and processes, the bank should keep in mind that OFAC considers the continued operation of an account or the processing of transactions post-designation, along with the adequacy of their OFAC compliance program, to be a factor in determining penalty actions.[130] The bank should maintain documentation of its OFAC checks on new accounts, the existing customer base and specific transactions.

If a bank uses a third party, such as an agent or service provider, to perform OFAC checks on its behalf, as with any other responsibility performed by a third party, the bank is ultimately responsible for that third party's compliance with the OFAC requirements. As a result, banks should establish adequate controls and review procedures for such relationships.

Updating OFAC lists. A bank's OFAC program should include policies, procedures, and processes for timely updating of the lists of blocked countries, entities, and individuals and disseminating such information throughout the bank's domestic operations and its offshore offices, branches and, in the case of Cuba and North Korea, foreign subsidiaries. This would include ensuring that any manual updates of interdiction software are completed in a timely manner.

Screening ACH transactions. All parties to an ACH transaction are subject to the requirements of OFAC. Refer to the expanded overview section, "Automated Clearing House Transactions," page 196, for additional guidance. OFAC has clarified the application of its rules for domestic and cross-border ACH transactions and is working with industry to provide more detailed guidance on cross-border ACH.[131]

With respect to domestic ACH transactions, the Originating Depository Financial Institution (ODFI) is responsible for verifying that the Originator is not a blocked party and making a good faith effort to determine that the Originator is not transmitting blocked funds. The Receiving Depository Financial Institution (RDFI) similarly is responsible for verifying that the Receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC policies. ODFIs are not responsible for unbatching transactions and ensuring that they do not process transactions in violation of OFAC's regulations if they receive those transactions already batched from their customers. If the ODFI unbatches the transactions it received from its customers, then the ODFI is responsible for screening as though it had done the initial batching.

---

[130] Interim final rule 31 CFR 501, "Economic Sanctions Enforcement Procedures for Banking Institutions," discusses that OFAC will take a bank-wide rather than a "per transaction" approach to enforcement. This methodology should consider risk-based efforts by banks to ensure OFAC compliance as well as evaluating violations. Further information is available on OFAC's web site www.treas.gov/ofac.

[131] See Interpretive Note 041214-FACRL-GN-02 at www.treas.gov/offices/enforcement/ofac/rulings/. NACHA rules further specify this compliance (see page 8 of the Quick Find section of the *2006 NACHA Operating Rules*).

With respect to OFAC screening, these same obligations hold for cross-border ACH transactions. For outbound cross-border ACH transactions, however, the ODFI cannot rely on OFAC screening by the RDFI outside of the United States. In the case of inbound ACH transactions, the RDFI is responsible for compliance with OFAC requirements.

Additional information on the types of retail payment systems (ACH payment systems) is available in the FFIEC *Information Technology Examination Handbook*.[132]

Reporting. An OFAC program should also include policies, procedures, and processes for handling items that are valid blocked or rejected items under the various sanctions programs. In the case of interdictions related to narcotics trafficking or terrorism, banks should notify OFAC as soon as possible by phone or e-hotline about potential hits with a follow-up in writing within ten days. Most other items should be reported through usual channels within ten days of the occurrence. The policies, procedures, and processes should also address the management of blocked accounts. Banks are responsible for tracking the amount of blocked funds, the ownership of those funds, and interest paid on those funds. Total amounts blocked, including interest, must be reported to OFAC by September 30 of each year (information as of June 30). When a bank acquires or merges with another bank, both banks should take into consideration the need to review and maintain such records and information.

Banks no longer need to file Suspicious Activity Reports (SARs) based solely on blocked narcotics- or terrorism-related transactions, as long as the bank files the required blocking report with OFAC. However, because blocking reports require only limited information, if the bank is in possession of additional information not included on the blocking report filed with OFAC, a separate SAR should be filed with FinCEN including that information. In addition, the bank should file a SAR if the transaction itself would be considered suspicious in the absence of a valid OFAC match.[133]

Maintaining license information. OFAC recommends that banks consider maintaining copies of customers' OFAC licenses on file. This will allow the bank to verify whether a customer is initiating a legal transaction. Banks should also be aware of the expiration date on the license. If it is unclear whether a particular transaction is authorized by a license, the bank should confirm with OFAC. Maintaining copies of licenses will also be useful if another bank in the payment chain requests verification of a license's validity. Copies of licenses should be maintained for five years, following the most recent transaction conducted in accordance with the license.

Independent Testing

Every bank should conduct an independent test of its OFAC program that is performed by the internal audit department, outside auditors, consultants, or other qualified

[132] The FFIEC *Information Technology Examination Handbook* is available at www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

[133] See FinCEN Release Number 2004-02, "Unitary Filing of Suspicious Activity and Blocking Reports," 69 *Federal Register* 76847, December 23, 2004.

independent parties. For large banks, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas. For smaller banks, the audit should be consistent with the bank's OFAC risk profile or be based on a perceived risk. The person(s) responsible for testing should conduct an objective, comprehensive evaluation of OFAC policies, procedures, and processes. The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC program.

Responsible Individual

It is recommended that every bank designate a qualified individual(s) to be responsible for the day-to-day compliance of the OFAC program, including the reporting of blocked or rejected transactions to OFAC and the oversight of blocked funds. This individual should have an appropriate level of knowledge about OFAC regulations commensurate with the bank's OFAC risk profile.

Training

The bank should provide adequate training for all appropriate employees. The scope and frequency of the training should be consistent with the bank's OFAC risk profile and appropriate to employee responsibilities.

Examination Procedures

Office of Foreign Assets Control

Objective. *Assess the bank's risk-based Office of Foreign Assets Control (OFAC) program to evaluate whether it is appropriate for the bank's OFAC risk, taking into consideration its products, services, customers, transactions, and geographic locations.*

1. Determine whether the board of directors and senior management of the bank have developed policies, procedures, and processes based on their risk assessment to ensure compliance with OFAC laws and regulations.

2. Regarding the risk assessment, review the bank's OFAC program. Consider the following:

   - The extent of, and method for, conducting OFAC searches of each relevant department or business line (e.g., automated clearing house (ACH) transactions, monetary instrument sales, check cashing, trusts, loans, deposits, and investments) as the process may vary from one department or business line to another.
   - The extent of, and method for, conducting OFAC searches of account parties other than accountholders, which may include beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney.
   - How responsibility for OFAC is assigned.
   - Timeliness of obtaining and updating OFAC lists or filtering criteria.
   - The appropriateness of the filtering criteria used by the bank to reasonably identify OFAC matches (e.g., the extent to which the filtering or search criteria includes misspellings and name derivations).
   - The process used to investigate potential matches.
   - The process used to block and reject transactions.
   - The process used to inform management of blocked or rejected transactions.
   - The adequacy and timeliness of reports to OFAC.
   - The process to manage blocked accounts (such accounts are reported to OFAC and pay a commercially reasonable rate of interest).
   - The record retention requirements (i.e., five-year requirement to retain relevant OFAC records; for blocked property, record retention for as long as blocked; once unblocked, records must be maintained for five years).

3. Determine the adequacy of independent testing (audit) and follow-up procedures.

4. Review the adequacy of the bank's OFAC training program based on the bank's OFAC risk assessment.

5. Determine whether the bank has adequately addressed weaknesses or deficiencies identified by OFAC, auditors, or regulators.

Transaction Testing

6. On the basis of a bank's risk assessment, prior examination reports, and a review of the bank's audit findings, select the following samples to test the bank's OFAC program for adequacy, as follows:

   - Sample new accounts (e.g., deposit, loan, trust, safe deposit, investments, credit cards, and foreign office accounts,) and evaluate the filtering process used to search the OFAC database (e.g., the timing of the search), and documentation maintained evidencing the searches.

   - Sample appropriate transactions that may not be related to an account (e.g., funds transfers, monetary instrument sales, and check-cashing transactions), and evaluate the filtering criteria used to search the OFAC database, the timing of the search, and documentation maintained evidencing the searches.

   - If the bank uses an automated system to conduct searches, assess the timing of when updates are made to the system, and when the most recent OFAC changes were made to the system. Also, evaluate whether all of the bank's databases are run against the automated system, and the frequency upon which searches are made. If there is any doubt regarding the effectiveness of the OFAC filter, then run tests of the system by entering test account names that are the same as or similar to those recently added to the OFAC list to determine whether the system identifies a potential hit.

   - If the bank does not use an automated system, evaluate the process used to check the existing customer base against the OFAC list and the frequency of such checks.

   - Review a sample of potential OFAC matches and evaluate the bank's resolution for blocking and rejecting processes.

   - Review a sample of reports to OFAC and evaluate their completeness and timeliness.

   - If the bank is required to maintain blocked accounts, select a sample and evaluate that the bank maintains adequate records of amounts blocked and ownership of blocked funds, that the bank is paying a commercially reasonable rate of interest on all blocked accounts, and that it is accurately reporting required information annually (by September 30th) to OFAC. Test the controls in place to verify that the account is blocked.

- Pull a sample of false hits (potential matches) to check their handling; the resolution of a false hit should take place outside of the business line.

7. Identify any potential matches that were not reported to OFAC, discuss with bank management, advise bank management to immediately notify OFAC of unreported transactions, and immediately notify supervisory personnel at your regulatory agency.

8. Determine the origin of deficiencies (e.g., training, audit, risk assessment, internal controls, management oversight), and conclude on the adequacy of the bank's OFAC program.

9. Discuss OFAC related examination findings with bank management.

10. Include OFAC conclusions within the report of examination, as appropriate.